CII WHITE PAPER

Defizite, Anforderungen und Maßnahmen:

# Kommunale Cybersicherheit auf dem Prüfstand

Rechtsanwalt Dr. Tilmann Dittrich, LL.M.
Prof. Dr. Dennis-Kenji Kipker

Powered by: NordPass®

CYBER|NTELLIGENCE .Institute

# Inhalt

# Die Autoren der Studie

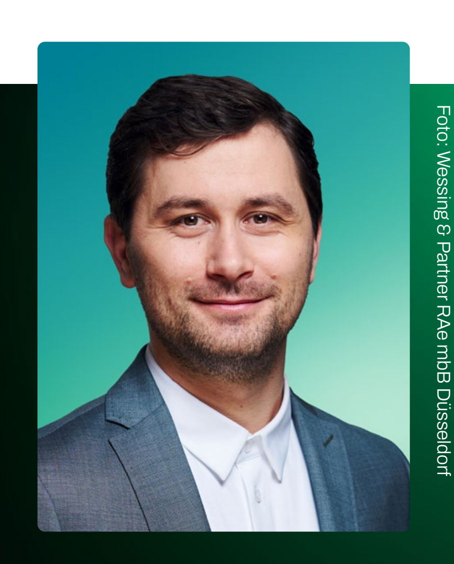


Foto: Wessing & Partner RAe mbB Düsseldorf

## Dr. Tilmann Dittrich, LL.M.

Dr. Tilmann Dittrich, LL.M. Medizinrecht, war Doktorand an der Heinrich-Heine-Universität Düsseldorf und hat dort zu Compliance-Herausforderungen im Non-Profit-Bereich geforscht. Er ist außerdem Rechtsanwalt in Düsseldorf.

Im Jahr 2024 hat er zwei juristische Fachbücher zur Krisenresilienz und Cybersicherheit im Gesundheitswesen mitherausgegeben, außerdem ist er Autor zahlreicher Publikationen zu den Themen Cybersecurity, Compliance und Strafrecht.



Foto: Urban Zintel Photography, Berlin

## Prof. Dr. Dennis Kenji Kipker

Prof. Dr. Dennis-Kenji Kipker ist wissenschaftlicher Direktor des cyberintelligence.institute in Frankfurt a.M., Vorstand der Strategieberatungsgesellschaft CERTAVO AG sowie Gastprofessor an der privaten, durch die Soros Foundation begründeten Riga Graduate School of Law in Lettland. Hier forscht er zu Themen an der Schnittstelle von Recht und Technik in der Cybersicherheit, Konzernstrategie sowie zu digitaler Resilienz im Kontext globaler Krisen mit einem Forschungsschwerpunkt insbesondere im chinesischen und US-amerikanischen IT-Recht.

# Executive Summary

Das vorliegende Gutachten untersucht den Status quo der kommunalen Cybersicherheit in Deutschland aus juristischer sowie organisatorischer Perspektive und zeigt Verbesserungsmöglichkeiten vor dem Hintergrund zahlreicher erfolgreicher Cyberangriffe auf. In verschiedenen öffentlichen Lageberichten wird die Gefährdungslage für Kommunen im Bereich der Cybersicherheit als ernst bewertet. Die Angriffe reichen von kleinen Gemeinden bis zu Großstädten und führen teilweise zu wochenlangen Ausfällen wichtiger Verwaltungsdienstleistungen.

Rechtlich wird die kommunale Cybersicherheit durch verschiedene Regelwerke tangiert, sie ist aber nicht umfassend geregelt. Die DSGVO verpflichtet zur Ergreifung technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten. Das BSIG fokussiert auf die Funktionsfähigkeit kritischer Infrastrukturen, die auch in der Hand von Kommunen sein können. Zusätzlich haben einige Bundesländer eigene IT-Sicherheits- oder Cybersicherheitsgesetze erlassen, die teilweise auch Kommunen erfassen.

**Die Cybersicherheitsarchitektur in Deutschland, insbesondere auf Länder- und Kommunalebene, wird vielfach als „Wimmelbild“ mit nur schwer überschaubaren Zuständigkeiten bezeichnet.**

Trotz dieser Regelungen bestehen erhebliche Verbesserungspotenziale. Die Cybersicherheitsarchitektur in Deutschland, insbesondere auf Länder- und Kommunalebene, wird vielfach als „Wimmelbild“ mit nur schwer überschaubaren Zuständigkeiten bezeichnet – zugegebenermaßen steht Deutschland mit einer verteilten nationalen Cybersicherheitsarchitektur in der Europäischen Union aber nicht allein da. Es fehlt nach wie vor an umfassenden Regelungen, die Kommunen ganzheitlich zur Resilienz verpflichten. Hier sind vor allem die Bundesländer am Zug.

Bis rechtliche Nachbesserungen erfolgt sind, müssen die Kommunen weiterhin eigeninitiativ tätig werden, um ihre Cybersicherheit zu stärken. Der Leitungsebene von Kommunen kommt hier eine herausragende Bedeutung zu, denn sie trägt die Letztverantwortung für den Cybersicherheitsbereich. Sie ist trotz der engen finanziellen und personellen Ressourcen aber ebenso auf Fachpersonal innerhalb der Kommune angewiesen. Deshalb ist die Etablierung eines „Kommunal-CISO“ in fachlicher Hinsicht zu empfehlen. Überdies sind Standardisierungen für die Etablierung von Sicherheitskonzepten mit den dazugehörigen Sicherheitsmaßnahmen vorhanden. Diese umfassen auch die Vorbereitung auf einen Krisenfall, was unerlässlich ist.

# Teil 1
# Gefährdungslage

**Begriffsbestimmung Cybersicherheit**
Cybersicherheit dient als Oberbegriff für eine Reihe an Sicherheitskategorien und befasst sich generell mit der Sicherheit von Datenverarbeitungsvorgängen im vernetzten Raum.[1] Als Oberbegriff bestehen Schnittmengen mit der IT-Sicherheit, der Informationssicherheit sowie der Datensicherheit.

> **Cybersicherheit dient als Oberbegriff für eine Reihe an Sicherheitskategorien und befasst sich generell mit der Sicherheit von Datenverarbeitungsvorgängen im vernetzten Raum.**

Die IT-Sicherheit bezweckt die Sicherheit speziell in IT-Systemen, etwa vor Angriffen von außen. Insbesondere der Unterbegriff der IT-Sicherheit kann aber in einem ohnehin weitreichend vernetzten Raum nicht immer trennscharf von der Cybersicherheit abgegrenzt werden.[2]

Die Informationssicherheit ist weniger technisch konnotiert und umfasst die Sicherheit von in Daten enthaltenen Informationen, ohne aber auf den Inhalt dieser Informationen bewusst abzustellen. Dies hingegen erfolgt beim Begriff der Datensicherheit, da es hier um die Sicherheit von personenbezogenen Daten durch technische und organisatorische Schutzmaßnahmen geht.[3]

Typischerweise wird bei der Cybersicherheit auf drei verschiedene Schutzziele abgestellt, im Akronym auch als „CIA-Triade“ bezeichnet. Die Vertraulichkeit (Confidentiality) umfasst die Geheimhaltung von Informationen, die nur von autorisierten Personen gelesen werden dürfen. Die Integrität (Integrity) schützt Informationen, damit diese nicht unbefugt verändert werden können. Die Verfügbarkeit (Availability) ist deshalb schützenswert, damit die mit den IT-Systemen verarbeiteten Informationen stets zugreifbar sind und so die Dienste angeboten werden können.[4]

**Begriffsbestimmung Kommune**
Der ins Deutsche übersetzte Begriff der „Gemeinden“ für die Kommunen wird im Grundgesetz vor allem in Art. 28 GG aufgegriffen. Es handelt sich bei den Kommunen um einen Teil der demokratisch verfassten Staatsgewalt[5], nämlich einem Teil der Landesstaatsgewalt[6]. Die Gemeinden sind von der örtlichen Gemeinschaft legitimierte Gebietskörperschaften[7]. Laut BSI-Lagebericht 2022 gibt es in Deutschland knapp 11.000 Gemeinden.[8]

Art. 28 Abs. 2 S. 1 GG sichert den Gemeinden zu, alle Angelegenheiten der örtlichen Gemeinschaft im Rahmen der Gesetze in eigener Verantwortung zu regeln, was als gemeindliche Selbstverwaltungsgarantie bezeichnet wird. Dies umfasst im Kern die Weisungsfreiheit gegenüber staatlichen Institutionen, organisatorische Wahlmöglichkeiten sowie eine freie Alternativenwahl im Rahmen der Rechtsordnung.[9] Die Selbstverwaltungsgarantie umfasst auch die kommunalen Organisationsbefugnisse, enthält aber kein derartiges Prinzip der Eigenorganisation der Gemeinde, demgegenüber jede staatliche Vorgabe einer spezifischen Rechtfertigung bedürfe. So verbietet die Garantie Regelungen, die eine eigenständige organisatorische

1 Kipker, in: Kipker, Cybersecurity, Kap. 1 Rn. 4.
2 Kipker, in: Kipker, Cybersecurity, Kap. 1 Rn. 4.
3 Kipker, in: Kipker, Cybersecurity, Kap. 1 Rn. 4.
4 Sohr/Kemmerich, in: Kipker, Cybersecurity, Kap. 2 Rn. 6-10.
5 BVerfG, Urt. v. 4.11.1986 – 1 BvF 1/84, NJW 1987, 239 (248); BVerfG, Urt. v. 31.10.1990 – 2 BvF 2/89, 2 BvF 6/89, NJW 1991, 162 (164).
6 Hellermann, in: BeckOK GG, Art. 28 Rn. 21 m. w. N.; Herrmann/Stöber, NVwZ 2017, 1401 (1403); Rüdebusch, KommJur 2020, 41 (43).
7 Mehde, in: Dürig/Herzog/Scholz, GG, Art. 28 Rn. 172.
8 „Die Lage der IT-Sicherheit in Deutschland 2022“ des BSI, S. 87.
9 Hellermann, in: BeckOK GG, Art. 28 Rn. 42.

Gestaltungsfähigkeit der Kommunen im Ergebnis ersticken würden. Der Gesetzgeber hat den Gemeinden einen hinreichenden organisatorischen Spielraum bei der Wahrnehmung der je einzelnen Aufgabenbereiche offenzuhalten.[10]

Eine solche Selbstverwaltungsgarantie steht nach Art. 28 Abs. 2 S. 2 GG auch den Gemeindeverbänden zu. Hierzu zählen in erster Linie die Landkreise.[11] Keine Gemeindeverbände sind aufgrund ihres begrenzten Aufgabenkreises hingegen Zweckverbände[12], wie die im weiteren Verlauf dieser Studie thematisierte Südwestfalen-IT.

**Lageberichte zur Cybersicherheit von Kommunen**
Zur Einschätzung der Gefährdungslage von Kommunen sind Berichte von öffentlichen Stellen hilfreich. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt in seinem Lagebericht zur IT-Sicherheit in Deutschland für das Berichtsjahr 2023 (Berichtszeitraum vom 01.06.2022 bis zum 30.06.2023) an[13], durchschnittlich zwei Kommunalverwaltungen oder kommunale Betriebe seien monatlich von Ransomware-Angriffen betroffen. Bei dieser Angriffsart verschlüsseln die Täter Daten in den IT-Systemen der Opfer, was dort zu Betriebseinschränkungen führen kann, und kopieren diese, um mit deren Veröffentlichung ein weiteres Argument für eine Lösegeldzahlung zu aktivieren. Bei den Kommunen fänden überproportional häufig Ransomware-Angriffe statt.

> **Bei den Kommunen fänden überproportional häufig Ransomware-Angriffe statt.**

Die Angriffe hätten von kleinen Gemeinden mit 2.800 Einwohnern bis zu Großstädten mit mehr als 1 Million Einwohnern gereicht, insgesamt seien im Berichtsjahr etwa 6.000.000 Einwohner von solchen Angriffen auf ihre Kommunen betroffen gewesen.[14] Typische Auswirkungen solcher Angriffe seien die Leaks von personenbezogenen Daten. Teilweise seien die Kommunen mehrere Tage bis hin zu mehreren Wochen nicht in der Lage gewesen, ihre bürger- und wirtschaftsnahen Verwaltungsdienstleistungen zu erbringen, und teils noch Monate später beeinträchtigt gewesen.[15] Auch im Lage-




bericht 2024 (Berichtszeitraum vom 01.07.2023 bis zum 30.06.2024) spricht das BSI zusammenfassend davon, dass „Opfer (...) neben überwiegend kleinen und mittleren Unternehmen insbesondere IT-Dienstleister und auch wieder Kommunen“[16] waren.

Vereinzelt geben auch Länder Lageberichte heraus. Hier ist besonders das Land Hessen zu erwähnen. Das im Verlauf des Gutachtens noch thematisierte CyberCompetenceCenter („Hessen3C“) als Zentrum der Hessischen Cybersicherheitsarchitektur veröffentlichte im Januar 2025 seine Gefährdungsbeurteilung für das Jahr 2024.[17] Danach seien dem „Hessen3C“ im Jahr 2024 21 Cyberangriffe auf hessische Kommunen freiwillig gemeldet worden, bei denen in der Mehrzahl niedrigschwellige Angriffsformen genutzt worden seien, es daher keine Datenabflüsse oder ein komplettes Erliegen der Systeme gegeben habe, die Zahl der ernstzunehmenden Angriffe aber alarmierend hoch sei.

10 BVerfG, Beschl. v. 26.10.1994 – 2 BvR 445/91, NVwZ 1995, 677.
11 St. Rspr., vgl. BVerfG, Beschl. v. 15.12.2020 – 1 BvR 1395/19, NJW 2021, 1665 (1668 Rn. 37).
12 BVerwG, Urt. v. 23.08.2011 – 9 C 2/11, NVwZ 2012, 506 (507 f.); LVerfG Schleswig-Holstein, Urt. v. 26.02.2010 – LVerfG 1/09, NordÖR 2010, 155 (158).
13 „Die Lage der IT-Sicherheit in Deutschland 2023“ des BSI, S. 68.
14 „Die Lage der IT-Sicherheit in Deutschland 2023“ des BSI, S. 69.
15 „Die Lage der IT-Sicherheit in Deutschland 2023“ des BSI, S. 68.
16 „Die Lage der IT-Sicherheit in Deutschland 2024“ des BSI, S. 8 (kursive Hervorhebung durch die Autoren).
17 Pressemitteilung des Hessischen Ministeriums des Innern, für Sicherheit und Heimatschutz vom 03.01.2025.

**Ableitung aktueller Gefährdungslage von Kommunen und Prognosen**
Um die Schwachstellen der Cybersicherheit in Kommunen nun näher beurteilen zu können, müssen erfolgreiche Angriffe begutachtet werden. Hierfür kommen beispielhaft der Angriff auf den Landkreis Anhalt-Bitterfeld im Jahr 2021 sowie der Cyberangriff auf die Südwestfalen-IT im Jahr 2023 in Betracht.

Der Angriff auf den Landkreis Bitterfeld wird u.a. im BSI-Lagebericht 2022 ausführlich beschrieben, denn zum ersten Mal wurde in Deutschland aufgrund eines Cyber Incidents der Katastrophenfall durch einen Landkreis, also einen Gemeindeverbund, ausgerufen.[18] Vier Tage, nachdem der Angriff, der sämtliche IT-Systeme aller Standorte der Kreisverwaltung betraf, im Juli 2021 bekanntgeworden war, rief der Landkreis den Katastrophenfall aus. Erst Anfang Februar 2022 konnte dieser

> **Vier Tage, nachdem der Angriff, der sämtliche IT-Systeme aller Standorte der Kreisverwaltung betraf, im Juli 2021 bekanntgeworden war, rief der Landkreis den Katastrophenfall aus.**

wieder aufgehoben werden. Der Landkreis ging nicht auf die Lösegeldforderung ein, es erfolgte keine Veröffentlichung geleakter Daten im Darknet. In diesem Zusammenhang weist das BSI darauf hin, dass der Ausfall bzw. die erhebliche Beeinträchtigung der kommunalen Verwaltungsprozesse zu vielfältigen Belastungen innerhalb der Bevölkerung führen kann. Dies gelte besonders für Personengruppen, die möglicherweise durch ausbleibende Zahlungen, etwa von Sozialleistungen oder Elterngeld, unmittelbar vom Ausfall kritischer Dienstleistungen betroffen seien[19].

Ein weiterer signifikanter Angriff mit Auswirkungen auf Kommunen fand Ende 2023 auf die Südwestfalen-IT (SIT) statt, ein Bericht hierzu ist auch im BSI-Lagebericht 2024 veröffentlicht[20]. Hierbei handelt es sich um einen kommunalen IT-Dienstleister, der zum Zeitpunkt des Angriffs als Zweckverband die IT für 72 Kommunen voll oder zum Teil betrieb.[21] Der IT-Dienstleister veröffentlichte im Nachgang einen Bericht zum Vorfall, der einen Angriff über eine schwerwiegende Sicherheitslücke (fehlende Multi-Faktor-Authentifizierung) beschreibt. Nach eigenen Aussagen musste auf die Lösegeldforderung nicht eingegangen werden, da valide Sicherungskopien der verschlüsselten Daten vorlagen.[22] Der Cyberangriff verdeutlicht das Risiko von Angriffen in der digitalen Lieferkette, wenn also IT-Dienstleistungen an Dritte ausgelagert werden oder sich IT-Systeme aus Komponenten verschiedener Hersteller zusammensetzen. Die Auswirkungen des Angriffs waren immens. Erst im Juli 2024 gab das Unternehmen bekannt, die Online-Dienstleistungen für die betroffenen 1,7 Millionen Einwohner funktionierten nun wieder weitgehend fehlerfrei. In der Zwischenzeit mussten sich die Kommunen mit Notfall-Homepages, vermehrten Papierdokumenten und alternativen Kommunikationswegen helfen.[23]

**Ermittlung und Zusammenfassung der Gründe unzureichender kommunaler Cybersicherheit in Deutschland**
Zunächst steht fest, dass sämtliche Bereiche des gesellschaftlichen Lebens, in denen die Digitalisierung stattfindet, durch Cybervorfälle gefährdet sind.[24] Es gibt außerdem eine Reihe an für Kriminelle besonders attraktiven Zielen, bei denen man sich, etwa aufgrund der Kritikalität von Dienstleistungen oder der Verarbeitung hochsensibler Informationen, eine hohe „Zahlungsmoral" auf die Lösegeldforderung erhofft, was man als „Big Game Hunting" bezeichnet.[25] Als solches Beispiel dienen bspw. Krankenhäuser, da hier aufgrund der Gesundheitsgefahren und der Sensibilität der verarbeiteten personenbezogenen Daten ein hoher Zahlungsdruck aufgebaut werden kann. Dieser Anreiz des hohen Zahlungsdrucks aufgrund betriebsbeeinträchtigender Einschränkungen wirkt sich nur in Sonderkonstellationen auf Kommunen aus, wenn sie etwa solche kritischen

18 „Die Lage der IT-Sicherheit in Deutschland 2022" des BSI, S. 21.
19 „Die Lage der IT-Sicherheit in Deutschland 2022" des BSI, S. 21.
20 „Die Lage der IT-Sicherheit in Deutschland 2024", S. 75.
21 https://www1.wdr.de/nachrichten/westfalen-lippe/suedwestfalen-it-raeumt-sicherheitsluecke-ein-100.html.
22 „Abschlussbericht Security Incident – Südwestfalen-IT", S. 5.
23 https://www.heise.de/news/Neun-Monate-nach-Cyberangriff-Suedwestfalen-IT-ist-wieder-online-9812619.html.
24 „Die Lage der IT-Sicherheit in Deutschland 2023" des BSI, S. 11.
25 „Die Lage der IT-Sicherheit in Deutschland 2022" des BSI, S. 11.

Dienstleistungen erbringen. Grundsätzlich ist aber bei Kommunen mit keiner bedeutenden Zahlungsmoral zu rechnen. So wird in einem gemeinsam Hinweispapier des Deutschen Städtebunds, des Deutschen Landkreistags und des Deutschen Städte- und Gemeindebunds in Zusammenarbeit mit dem BSI und dem Bundeskriminalamt davon abgeraten, auf Lösegeldforderungen einzugehen.[26] Mit einem Ausreißer der Gemeinde Dettelbach in Bayern im Jahr 2016 fehlt es auch an Berichten über Lösegeldzahlungen durch Gemeinden.[27]

Daher kommen anderweitige Anreize für Cyberangriffe auf Kommunen in Betracht. Diese liegen zum einen darin, dass sich mit den erbeuteten Daten hohen finanzielle Erlöse erzielen lassen. Zum anderen üben Gemeinden Staatsgewalt[28] aus und sind daher für Hacktivismus-Kampagnen relevant.[29] Hierbei verfolgen Cyberkriminelle, die oftmals staatliche Unterstützung erhalten oder unmittelbar einem Staat zuzuordnen sind, nicht primär wirtschaftliche, sondern vielmehr politische Ziele – dies insbesondere auch in Zeiten von Desinformation und hybrider Wahlbeeinflussung. Als weiteren Anreiz gelten

> **Hierbei verfolgen Cyberkriminelle, die oftmals staatliche Unterstützung erhalten oder unmittelbar einem Staat zuzuordnen sind, nicht primär wirtschaftliche, sondern vielmehr politische Ziele.**

staatliche Einrichtungen als finanziell nur geringfügig ausgestattet, was dafür spricht, dass auch ihre Investitionen in die Cybersicherheit nicht umfassend sind und sie demnach leichte Opfer für die Angreifer sein können.

26 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Presse/Ransomware-Kommunen-Empfehlung.pdf?__blob=publicationFile&v=1.

27 https://www.egovernment.de/zum-ersten-mal-zahlt-eine-stadtverwaltung-loesegeld-a-523975/.

28 BVerfG, Urt. v. 31.10.1990 - 2 BvF 2/89, 2 BvF 6/89, BVerfGE 83, 37 (58).

29 Allgemein zum Hacktivismus: „Die Lage der IT-Sicherheit in Deutschland 2023“ des BSI, S. 45 f.

## Teil 3

# Rechtliche und organisatorische Rahmenbedingungen

Aufgrund der zuvor skizzierten ausgeprägten Gefährdungslage stellt sich die Frage nach der aktuellen rechtlichen Regulierung der Cybersicherheit für Kommunen, zudem werden weitere organisatorische Rahmenbedingungen ohne Gesetzescharakter analysiert.

**DSGVO**

Den größten Anwendungsbereich für die Regulierung der Cybersicherheit weist die DSGVO[30] auf. Denn ihr Anwendungsbereich ist nicht auf bestimmte Sektoren oder Dienste zugeschnitten, sondern gilt überall dort, wo personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO verarbeitet werden, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Für die Verarbeitung von personenbezogenen Daten stellt Art. 5 DSGVO verschiedene Grundsätze auf. Einer dieser Grundsätze ist nach Art. 5 Abs. 1 lit. f DSGVO der Grundsatz von „Integrität und Vertraulichkeit", der durch Art. 32 DSGVO konkretisiert wird.[31] Dieser verpflichtet die für die Datenverarbeitung verantwortliche Person (Art. 4 Nr. 7 DSGVO), technische und organisatorische Maßnahmen (TOM) zu ergreifen, um ein dem für die Daten bestehenden Risiko angemessenes Schutzniveau zu ergreifen. Maßgeblich ist also insbesondere die Sensibilität der verarbeiteten Daten. Art. 32 Abs. 1 DSGVO nennt als TOM beispielhaft vier verschiedene Sicherheitsmaßnahmen:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Verarbeitet werden bei einer Kommune die personenbezogenen Daten von Bürgern. Auch wenn eine juristische Person, etwa bei der Anmeldung eines Gewerbes, der Kommune gegenübertritt, werden regelmäßig personenbezogene Daten der dahinterstehenden natürlichen Personen übermittelt und verarbeitet. Nicht zu vernachlässigen sind zudem die personenbezogenen Daten von Mitarbeitenden, die von der Kommune beschäftigt werden. Sowohl von Bürgern als auch Mitarbeitenden können die Daten eine hohe Sensibilität erreichen, wenn zum Beispiel sensible Informationen über Gesundheitszustände und körperliche Eigenschaften wie Behinderungen verarbeitet werden. Der Tätigkeitsbe-

30 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 S. 1, ber. L 314 S. 72, 2018 L 127 S. 2 und 2021 L 74 S. 35).

31 Herbst, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, DS-GVO, Art. 5 Rn. 51.

richt 2023 der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg erwähnt etwa die Prüfung von Parkerleichterungen durch Schwerbehinderte durch die Stadt Potsdam. Besonders brisant in diesem Fall war, dass die Fahrerlaubnisbehörde diese Informationen zugleich nutzte, um die Fahreignung der Personen zu überprüfen. Hierin sah die Aufsichtsbehörde aufgrund des besonderen Schutzbedarfs der Gesundheitsdaten schwerwiegende Verstöße und verwarnte die Stadtverwaltung nach Art. 58 Abs. 2 lit. b DSGVO.[32]

Gerade dieser Fall macht deutlich, warum die DSGVO in kommunalen Kontext kein solches Argument zur Cybersicherheit aufweist wie bei privaten Unternehmen.[33] Denn es handelt sich hierbei um einen eklatanten Verstoß in systematischer Vorgehensweise, der bei privaten Datenverarbeitern wohl kaum nur mit einer Verwarnung geendet wäre, sondern zur Verhängung eines hohen Bußgelds nach Art. 83 DSGVO geführt hätte. Bußgelder gegen Behörden sind in Deutschland aber nicht möglich. So hat man hierzulande von der Öffnungsklausel in Art. 83 Abs. 7 DSGVO Gebrauch gemacht und die Verhängung von Geldbußen gegen Behörden und öffentliche Stellen über § 43 Abs. 3 BDSG ausgeschlossen. Damit bleibt den Datenschutzbehörden gegenüber öffentlichen Stellen „nur“ die Aufsicht, Sanktionen scheiden aus. Aus dem Tätigkeitsbericht geht auch hervor, wie eine solche Aufsicht in Bezug auf Kommunen und Cyberangriffe stattfinden kann: die Landesbehörde führte eine technisch-organisatorische Prüfung nach zwei Cyberangriffen (2020, 2022) auf die Stadtverwaltung Potsdam durch. Die Behörde bezeichnete die Ergebnisse ihrer Prüfung als ernüchternd, so fehlte es insbesondere an einem gültigen Informationssicherheitskonzept. Weiterhin verletzte die Stadt regelmäßig und zunächst ohne Begründung durch die Behörde gesetzte Fristen im Rahmen der Überprüfung.[34] Auch hier wird wieder deutlich, dass sich die Kommune glücklich schätzen konnte, für ein solches „Nachtatverhalten“ nicht sanktioniert werden zu können.

> **Damit bleibt den Datenschutzbehörden gegenüber öffentlichen Stellen „nur“ die Aufsicht, Sanktionen scheiden aus.**

Des Weiteren muss berücksichtigt werden, dass durch die DSGVO nur ein Teilbereich der Cybersicherheit reguliert wird, nämlich die Datensicherheit. Für diese sieht Art. 32 Abs. 1 lit. c DSGVO auch die bei den beliebten Ransomware-Angriffen zur Abwehr notwendige Business Continuity als wichtige TOM an, um der Gefahr von Betriebseinschränkungen der IT-Systeme Herr werden zu können. Allerdings reicht diese Regulierung nicht aus. Denn es werden in Kommunen auch vielfach Informationen ohne Personenbezug verarbeitet, die aber dennoch für einen kontinuierlichen Betrieb der Kommune elementar sind. Diese Gefahrenlage deckt die DSGVO nicht ab.

**BSIG**

Mit einer anderen Zielrichtung als die DSGVO reguliert das BSIG[35] den Bereich der Cybersicherheit, da es in dessen Anwendungsbereich im Schwerpunkt um die Funktionsfähigkeit von Unternehmen und öffentlichen Einrichtungen geht, deren Dienste für die Gesellschaft wichtig sind und daher vor Cybergefahren geschützt werden müssen. Das Gesetz nennt die Adressatenkategorien der Anbieter Digitaler Dienste (§ 2 Abs. 11, 12 BSIG), der Betreiber Kritischer Infrastrukturen (§ 2 Abs. 10 BSIG) sowie die Unternehmen im besonderen öffentlichen Interesse (§ 2 Abs. 14 BSIG), wobei nur die zweitgenannte Kategorie für die Cybersicherheit von Kommunen relevant ist.

Nach § 2 Abs. 10 S. 1 BSIG sind Kritische Infrastrukturen Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Das Nä-

32 „Tätigkeitsbericht Datenschutz 2023“ der Landesbeauftragten für Datenschutz und Akteneinsicht Brandenburg, S. 52 ff.
33 In diese Richtung auch: Ziegler, Tagesspiegel Background Cybersicherheit v. 29.02.2024.
34 „Tätigkeitsbericht Datenschutz 2023“ der Landesbeauftragten für Datenschutz und Akteneinsicht Brandenburg, S. 67 ff.
35 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) v. 14.08.2009 (BGBl. I S. 2821).

here regelt die auf §§ 2 Abs. 10 S. 10, 10 BSIG gestützte BSI-Kritisverordnung.[36]

Es wird direkt deutlich, dass kein Sektor Verwaltung oder Kommunen existiert. Allerdings können Kommunen dann in den Anwendungsbereich fallen, wenn sie Einrichtungen betreiben, die den genannten Sektoren zugeordnet werden können. Dies gilt u.a. für den Sektor Energie, wenn Kommunen etwa Stadtwerke betreiben, wobei hier auch die Spezialvorschriften des EnWG zu berücksichtigen sind, aber auch für den Bereich der Gesundheit, wenn kommunale Krankenhäuser betrieben werden. Hierfür gelten die Konkretisierungen und Schwellenwerte aus der BSI-Kritisverordnung mit ihren Anhängen für die einzelnen Sektoren. Zu solchen kommunalen Kritis-Unternehmen zählen also größere Energieversorger, kommunale Krankenhäuser oder Organisationen der Siedlungsabfallversorgung.[37] Das BSI selbst hat den Autoren dieser Studie aus Sicherheitsgründen keine konkreten Zahlen zu den Kritis-Betreibern genannt, an denen Kommunen beteiligt sind.[38] Es ist hier aber von einer großen Betroffenheit auszugehen.

**Sofern für kommunale Unternehmen der Anwendungsbereich für Kritische Infrastrukturen eröffnet ist, sind diese nach § 8a Abs. 1, 1a BSIG zur Etablierung von Risikomanagement-Prozessen zur Vermeidung von Störungen ihrer IT mit Auswirkung auf die erbrachten Dienstleistungen verpflichtet.**

Sofern für kommunale Unternehmen der Anwendungsbereich für Kritische Infrastrukturen eröffnet ist, sind diese nach § 8a Abs. 1, 1a BSIG zur Etablierung von Risikomanagement-Prozessen zur Vermeidung von Störungen ihrer IT mit Auswirkung auf die erbrachten Dienstleistungen verpflichtet. Diesbezüglich gilt nach § 8a Abs. 3 BSIG eine Nachweispflicht sowie nach § 8a Abs. 4 BSIG die Prüfmöglichkeit durch das BSI. Zur besseren Kommunikation mit dem BSI muss nach § 8b Abs. 3 BSIG eine Registrierung der Kritischen Infrastruktur sowie eine Benennung einer Kontaktstelle gegenüber dem BSI erfolgen. Außerdem gilt eine Meldepflicht bei Störungen nach § 8b Abs. 4 BSIG.

Das BSI selbst erteilt zur Anzahl der bei ihm registrierten Unternehmen, die in kommunaler Hand stehen, aus Geheimhaltungsgründen keine Auskunft.[39] Es ist aber davon auszugehen, dass von den 1.119 beim BSI registrierten Betreibern Kritischer Infrastrukturen[40] eine nicht zu unterschätzende Anzahl in der Hand von Kommunen ist bzw. diese hieran beteiligt sind. Somit führt das BSIG nur in den Konstellationen, in denen die kommunalen Unternehmen die Schwellenwerte der BSI-KritisV erreichen dazu, dass deren Leistungserbringung besonders krisenresilient gewährleistet sein muss.

Diese Zahlen betroffener (kommunaler) Unternehmungen dürften künftig steigen. Denn die EU hat mit der EU-Cybersicherheitsstrategie[41] aus dem Jahr 2020 zwei Richtlinien auf den Weg gebracht, die 2022 in Kraft getreten sind und bis Oktober 2024 in allen europäischen Mitgliedstaaten hätten umgesetzt werden müssen[42]. Die NIS-2-Richtlinie[43] löst die bisherige NIS-Richtlinie zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen[44] ab und wird in Deutschland über das NIS2UmsuCG[45] im BSIG umgesetzt werden, im Ok-

36 „BSI-Kritisverordnung vom 22.04.2016 (BGBl. I S. 958).

37 Vogel/Ziegler, ICLR 1/2023, 1 (12) verweisen aber darauf, dass bestimmte Sektoren, wie etwa die Wasserversorgung, durch kleine kommunale Versorger geprägt seien, die die Schwellenwerte der BSI-Kritisverordnung selten überschreiten würden.

38 Eine Anfrage vom 02.08.2024 an das BSI wurde am 06.08.2024 dahingehend beantwortet, dass es sich „hier um vertrauliche Informationen (handelt), die einem besonderen Schutz unterliegen und daher weder veröffentlicht noch an nicht autorisierte Kreise verteilt werden dürfen".

39 So die Auskunft der Pressestelle des BSI auf eine Anfrage nach dem IFG durch den Autor Dittrich vom 01.08.2024 („Es handelt sich hier um vertrauliche Informationen, die einem besonderen Schutz unterliegen und daher weder veröffentlicht noch an nicht autorisierte Kreise verteilt werden dürfen.").

40 Vgl. die Zahlen zu den Kritis-Betreibern des BSI, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html.

41 https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-strategy.

42 Siehe dazu im europäischen Ländervergleich auch die Studie von Kipker, NIS2 in a European country comparison: How are the member states implementing the new EU cybersecurity legislation, https://cdn.prod.website-files.com/65d3147399d4240558e8d053/66f18d81e2948bb481064786_ABB%20NIS2%20EU%20Country%20Comparison%20Study.pdf (Stand: 24.09.2024).

43 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333/80).

44 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 S. 1, ber. ABl. 2018 L 33 S. 5).

45 NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz; die bisherigen Entwürfen zum NIS2UmsuCG sind gesammelt abrufbar unter: https://ag.kritis.info/2024/03/07/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/.

tober 2024 wurde das Gesetzesvorhaben erstmalig im Bundestag beraten, der weitere Fortgang war aufgrund der politischen Entwicklungen bislang nicht absehbar. Es wird damit gerechnet, dass künftig etwas unter 30.000 Unternehmen und öffentliche Einrichtungen vom künftigen BSIG erfasst werden. Doch auch hier wird eine unmittelbare Anwendbarkeit auf Kommunen fehlen. Für den entsprechenden Anwendungsbereich der NIS-2-Richtlinie sieht Art. 2 Abs. 5 lit. a NIS-2-RL eine Öffnungsklausel dahingehend vor, dass die Mitgliedsstaaten Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene ebenfalls verpflichten können. Von dieser Möglichkeit beabsichtigt aber der Bundesgesetzgeber zumindest keinen Gebrauch zu machen. Dies hat der IT-Planungsrat Bund und Ländern im November 2023 entsprechend empfohlen.[46]

Als zweite Richtlinie ist die Resilienz-Richtlinie verabschiedet worden, sie soll in einem KRITIS-DachG (KRITIS-Dachgesetz) umgesetzt werden[47]. Auch der hierzu veröffentlichte Regierungsentwurf wurde nicht mehr verabschiedet.[48] Das künftige KRITIS-DachG soll sich den physischen Gefahren für wichtige und besonders wichtige Einrichtungen widmen, weshalb man durch das beabsichtigte Zusammenspiel von BSIG und KRITIS-DachG von einem „All-Gefahren-Ansatz“[49] spricht, weil sich Gefahrenlagen mittlerweile oft nicht mehr klar in den cyber- oder nicht-cyber-bezogenen Gefahrenbereich einteilen lassen. Hierbei wird auch von der „hybriden Bedrohungslage“ gesprochen.

**Hierbei wird auch von der „hybriden Bedrohungslage“ gesprochen.**

**OZG mit Verordnung Portalverbund**

Seit 2017 gilt das Onlinezugangsgesetz, kurz OZG[50]. Hauptziel des Gesetzes ist es, den elektronischen Gang zur Behörde in Deutschland unkompliziert und sicher zu gestalten.[51] Hierfür werden Verwaltungsportale auf Bundes- und Landesebene aufgebaut und zu Portalverbünden zusammengeschlossen.[52] Eine Vielzahl an Verwaltungsleistungen muss dann über diese Portalverbünde durchgeführt werden.[53] Das OZG wurde im Juli 2024 umfassend durch das OZGÄndG[54] erneuert. In der ursprünglichen Fassung des OZG war umstritten[55], ob das Gesetz auch für Kommunen greift. Durch den neuen § 1 Abs. 1 Nr. 2 OZG ist nun aber klargestellt, dass der Anwendungsbereich für Verwaltungsleistungen der öffentlichen Stellen der Länder, einschließlich der Gemeinden und Gemeindeverbände, eröffnet ist.

§ 2 Abs. 1 OZG definiert Portalverbünde als eine technische Verknüpfung der Verwaltungsportale von Bund und Ländern, über den der Zugang zu Verwaltungsleistungen auf unterschiedlichen Portalen angeboten wird. Ein Verwaltungsportal bezeichnet nach § 2 Abs. 2 OZG ein bereits gebündeltes elektronisches Nutzungsangebot mit entsprechenden Angeboten einzelner Behörden.

Von IT-sicherheitsrechtlicher Relevanz sind im OZG die Vorschriften der §§ 4 bis 6 OZG. § 4 Abs. 1 OZG betrifft den Einsatz bestimmter IT-Komponenten und eine diesbezügliche Verordnungsermächtigung für die Bundesregierung im Benehmen mit dem IT-Planungsrat, § 6 Abs. 1 OZG soll für Sicherheitsstandards bei der Kommunikation zwischen den technischen Einrichtungen des Portalverbundes sorgen[56], indem das Bundesministerium des Innern und für Heimat (BMI) im Einvernehmen mit dem IT-Planungsrat durch Rechtsverordnung Sicherheitsstandards vorgibt.

46 https://www.it-planungsrat.de/beschluss/beschluss-2023-39.
47 Kipker/Dittrich, ZRP 2023, 230; Irmscher, ZRP 2024, 158.
48 BT-Drs. 20/13961
49 KRITIS-DachG-RefE, S. 1.
50 Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) v. 14.08.2017 (BGBl. I S. 3122, 3138).
51 Denkhaus/Richter/Bostelmann, in: Denkhaus/Richter/Bostelmann, OZG, § 1 Rn. 35.
52 Denkhaus/Richter/Bostelmann, in: Denkhaus/Richter/Bostelmann, OZG, § 1 Rn. 35.
53 Herrmann/Stöber, NVwZ 2017, 1401 (1403 f.); Lutz, in: Kipker, Cybersecurity, 15. Kap. Rn. 41.
54 Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG) v. 19.07.2024 (BGBl. 2024 I Nr. 245).
55 Denkhaus/Richter/Bostelmann, in: Denkhaus/Richter/Bostelmann, OZG, § 1 Rn. 11; Herrmann/Stöber, NVwZ 2017,1401 (1403); Rüdebusch, KommJur 2020, 41 (43).
56 Denkhaus/Richter/Bostelmann, in: Denkhaus/Richter/Bostelmann, OZG, § 6 Rn. 3.

Besonders bedeutsam ist nun § 5 OZG, der die IT-Sicherheit von Portalverbünden und den zur Anbindung an den Portalverbund genutzten IT-Komponenten betrifft. Hierfür werden die zur Gewährleistung der IT-Si-

> **Besonders bedeutsam ist nun § 5 OZG, der die IT-Sicherheit von Portalverbünden und den zur Anbindung an den Portalverbund genutzten IT-Komponenten betrifft.**

cherheit erforderlichen Standards durch das BMI ohne Zustimmung des Bundesrats festgelegt, nach § 5 S. 2 OZG ist die Einhaltung der IT-Sicherheitsstandards für alle Stellen verbindlich, die entsprechende IT-Komponenten nutzen. Die genannte Rechtsverordnung wurde im Januar 2022 erlassen.[57] Kernbestandteile des in der Verordnung festgelegten IT-Sicherheitsstandards nach § 2 ITSiV-PV sind[58]:

- Sicherheitsmaßnahmen nach dem Stand der Technik mit gesetzlicher Vermutung dieses Standards über vier Technische Richtlinien des BSI als Anlage der Verordnung (BSI TR-03160 „Servicekonten"; BSI TR-03107-1 „Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1"; BSI TR-03147 „Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen"; BSI TR-03116-4 „Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4");
- IT-Komponenten müssen einem Informationssicherheitsmanagement-System unterliegen, das die Vorgaben der gültigen Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrates umsetzt;
- Umsetzung eines IT-Sicherheitskonzepts durch die für die genutzten IT-Komponenten verantwortlichen Stellen, das den BSI-Standards 200-1 („Managementsysteme für Informationssicherheit"), 200-2 („IT-Grundschutz-Methodik") und 200-3 („Risikomanagement") oder der ISO 27001 („Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen") entspricht, wobei als Mindestanforderung die Umsetzung der Standard-Absicherung nach BSI-Standard 200-2 gilt;
- Penetrationstests für besonders sicherheitsrelevante IT-Komponenten;
- IT-Notfallmanagement für die genutzten IT-Komponenten nach der Leitlinie des IT-Planungsrates für die Informationssicherheit in der öffentlichen Verwaltung.




Aus unabhängigen Fachkreisen wurde allerdings erhebliche Kritik an der Rechtsverordnung geübt. So wird kritisiert, dass die Referenz auf die vier Technischen Richtlinien des BSI nicht ausreiche, da diese nicht das gesamte Spektrum der IT-Sicherheit abbildeten. Zudem sei der Standard für das Notfallmanagement durch die Verweisung auf den IT-Grundschutz nicht ausreichend, eine Referenz auf den BSI-Standard 200-4 bzw. die ISO-Norm 22301 für ein vollständiges Business-Continuity-Management wäre deutlich geeigneter gewesen.[59]

Unabhängig vom ausreichenden Standard in der ITSiV-PV betreffen die Sicherheitsvorgaben des OZG nur ausgewählte Verwaltungsleistungen von Kommunen. Sie führen nicht dazu, dass ein ganzheitliches Informationssicherheit-Management-System oder ein Business-Continuity-Management-System für die gesamte Kommune eingeführt werden müssen.

57 Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (IT-Sicherheitsverordnung Portalverbund – ITSiV-PV) v. 06.01.2022 (BGBl. I S. 18).

58 Lutz, in: Kipker, Cybersecurity, 15. Kap. Rn. 46.

59 https://ag.kritis.info/2022/01/25/bmi-rettet-die-fristgemaesse-umsetzung-des-ozg-durch-schwaechstmoegliche-verordnung-zur-it-sicherheit/.

## Länderregelungen




Neben den vorgenannten Regelwerken existiert mittlerweile auf Länderebene eine Reihe an Regelungen zur Cybersicherheit in Kommunen. Nachfolgend vorgestellt werden die Regelungen aus Baden-Württemberg, Hessen, Sachsen, Saarland, Bayern, Niedersachsen und Rheinland-Pfalz. Keine Regelungen getroffen haben bislang z. B. „Brandenburg, Bremen, Mecklenburg-Vorpommern, Thüringen und Sachsen-Anhalt“[60]. Lediglich eine Empfehlung für Kommunen stellt die „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ des IT-Planungsrats dar, die über das Regelungsinstrument des IT-Staatsvertrags verbindliche Anforderungen für Behörden und Einrichtungen der Verwaltungen des Bundes und der Länder darstellt.[61]

### 1) Cybersicherheitsgesetz Baden-Württemberg

Im Februar 2021 wurde in Baden-Württemberg das erste deutsche, ausdrücklich so benannte Cybersicherheitsgesetz[62] eines Landes verkündet. Danach wurde gemäß § 1 CSG BW eine Cybersicherheitsagentur mit Sitz in Stuttgart eingerichtet, die für die Cybersicherheit in Baden-Württemberg zuständig ist. Zuzuordnen ist die Behörde nach § 1 Abs. 3 CSG BW dem Innenministerium Baden-Württembergs, das die Dienst- und Fachaufsicht führt, es handelt sich also, wie auch beim BSI, nicht um eine unabhängige Sicherheitsbehörde[63]. Das Gesetz liefert in § 2 CSG BW die notwendigen Begriffsbestimmungen, bspw. zum Cyberraum, zur Cybersicherheit oder auch zur IT-Sicherheit.

Hauptaufgabe der Cybersicherheitsagentur ist nach § 3 Abs. 1 S. 1 CSW BW die Förderung der Cybersicherheit und der mit dieser zusammenhängenden Aspekte. Hierzu zählen insbesondere die Abwehr von Gefahren für die Cybersicherheit, der Schutz gesellschaftlicher Prozesse vor Angriffen im Cyberraum oder auch die Mitwirkung an der Entwicklung und Setzung von Standards für die Cybersicherheit der öffentlichen Stellen des Landes und der an das Landesverwaltungsnetz angeschlossenen Stellen. Zu den öffentlichen

> **Hierzu zählen insbesondere die Abwehr von Gefahren für die Cybersicherheit, der Schutz gesellschaftlicher Prozesse vor Angriffen im Cyberraum oder auch die Mitwirkung an der Entwicklung und Setzung von Standards für die Cybersicherheit der öffentlichen Stellen des Landes und der an das Landesverwaltungsnetz angeschlossenen Stellen.**

Stellen gehören nach § 2 Abs. 1 S. 1 CSG BW sowohl die Gemeinden als auch die Gemeindeverbände. Die Cybersicherheitsagentur übernimmt zudem beratende Aufgaben und bietet nach § 3 Abs. 2 CSG BW auf Ersuchen der erfassten Stellen Unterstützung bei der Abwehr von Gefahren für die Cybersicherheit oder verweist auf qualifizierte sicherheitsdienstleistende Personen. Diese Aufgabe ist bereits für das BSI nach § 5b BSIG[64] bekannt.

Die Cybersicherheitsagentur kann nach § 5 CSG BW gegenüber den erfassten Stellen Anordnungen zur Gefahrenabwehr treffen. Weiterhin sieht § 4 Abs. 3 S. 1 CSG BW eine unverzügliche Meldepflicht der betroffenen Stellen an die Cybersicherheitsagentur bei Sicher-

60 Martini/Botta, LKV 2024, 293 (294); zu Sachsen-Anhalt der Hinweis auf das Pilotprojekt „SicherKommunal in Sachsen-Anhalt“, Informationen abrufbar unter: https://www.mdr.de/nachrichten/sachsen-anhalt/it-sicherheit-kommunen-pilot-projekt-100.html.

61 „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ des IT-Planungsrats, Stand 2018, S. 5.

62 Gesetz für die Cybersicherheit in Baden-Württemberg (Cybersicherheitsgesetz – CSG) v. 04.02.2021 (GBl. S.182).

63 Dickmann/Vettermann, MMR 2022, 740 (744).

64 § 11 BSIG-E in der Fassung des Regierungsentwurfs des NIS2UmsuCG.

heitslücken im Sinne des § 4 Abs. 2 Nr. 1 i. V. m. § 2 Abs. 13 CSG BW vor.

Das Gesetz sieht somit im Ergebnis vor allem Eingriffsbefugnisse der Cybersicherheitsagentur zur Gefahrenabwehr vor, trifft aber keine weitreichenden Regelungen für die Gemeinden und Gemeindeverbände, wie diese selbst schon zur Gefahrvermeidung verpflichtet werden.

### 2) Hessisches IT-Sicherheitsgesetz (HITSiG)

Im Jahr 2023 ist das Hessische Gesetz zum Schutz der elektronischen Verwaltung[65] – auch Hessisches IT-Sicherheitsgesetz (HITSiG) genannt – in Kraft getreten. Damit reagierte das Land Hessen auf die Gefährdungslage für die öffentliche Verwaltung und bestätigte die Einschätzung der Bundesregierung, dass es sich bei der Gewährleistung der Cybersicherheit um eine gesamtstaatliche Aufgabe handle, die nur gelingen könne, wenn Bund, Länder und Kommunen eng zusammenarbeiteten[66].

Erstes Kernelement des Gesetzes ist das Cyber Competence Center (Hessen3C) als Zentralstelle zur Erhöhung der IT-Sicherheit in der Landesverwaltung und zur Abwehr von Gefahren für die Informationstechnik des Landes, das eigenständig, also ohne Amtshilfeersuchen anderer Landesbehörden, operativ tätig werden kann. Das Aufgabenspektrum von Hessen3C reicht von der Prävention durch Lagebeobachtung, Sammlung und Auswertung von Informationen zu Sicherheitsrisiken, Schwachstellen und Schadprogrammen, über Informationen, Warnungen und Empfehlungen an Behörden und auch an die Öffentlichkeit bis hin zur aktiven Abwehr von konkreten Gefahren.[67] Diese Zentralstellenfunktion ist in § 5 HITSiG geregelt.

Als zweites Kernelement fungiert ein Zentraler Informationssicherheitsbeauftragter der Landesverwaltung, auch als Chief Information Security Officer/CISO des Landes Hessen bezeichnet, nach § 4 HITSiG. Der CISO übernimmt in der Landesverwaltung eine überwachende und koordinierende Rolle, § 4 Abs. 1 S. 2 HITSiG.

Der Anwendungsbereich des Gesetzes erfasst nach § 1 Nr. 3 HITSiG auch die Verwaltungstätigkeit mittels Informationstechnik der Behörden und sonstigen öffentlichen Stellen der Gemeinden und Gemeindeverbände sowie nicht öffentlicher Stellen, soweit sie hoheitliche Aufgaben unter Aufsicht des Landes wahrnehmen. Für Kommunen und sonstige Stellen kann das Hessen3C im Wege der Auftragsverarbeitung entsprechende Dienstleistungen (je nach Kapazitäten) erbringen.[68] Außerdem kann etwa das Hessen3C im Falle einer IT-Störung von herausgehobener Bedeutung Maßnahmen treffen und Hilfestellungen für Kommunen geben, §§ 5 Abs. 2 S. 1 Nr. 4, 16 HITSiG.

### 3) Sächsisches Informationssicherheitsgesetz

Bereits 2019 hat das Land Sachsen ein Sächsisches Informationssicherheitsgesetz[69] eingeführt, das 2024 erneut überarbeitet wurde[70]. Nach § 1 S. 1 SächsISichG zielt das Gesetz darauf ab, die Informationssicherheit im Freistaat Sachsen zu erhöhen und Gefahren für informationstechnische Systeme abzuwehren. Das Gesetz gilt für die Behörden und die Gerichte des Freistaates Sachsen (staatliche Stellen) sowie die seiner Aufsicht unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (nicht-staatliche Stellen), erfasst sind somit auch die Kommunen.

Auch in Sachsen gibt es einen Beauftragten für Informationssicherheit des Landes (§ 5 Abs. 1 SächsISichG) sowie ein Sicherheitsnotfallteam (§ 6 SächsISichG).

Für die interne Sicherheitsorganisation sollen nicht-staatliche Stellen, zu denen Kommunen zählen, nach § 8 Abs. 1 SächsISichG einen Informationssicherheitsbeauftragten ernennen, der nicht zwingend Beschäftigter der nicht-staatlichen Stelle sein muss. Dies ermöglicht auch die Vergabe an externe IT-Sicherheits-Unternehmen. Strukturell ist zudem § 11 SächsISichG relevant, der die Datenübermittlung von nicht-staatlichen Stellen regelt. Die IT-Sicherheit soll dadurch gewahrt werden, dass entweder ein Zugang der Kommunen über das Kommunale Datennetz oder alternativ der

65 Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG) vom 29. Juni 2023 (GVBl. S. 433).

66 LT-Drs. 20/10752, S. 1.

67 LT-Drs. 20/10752, S. 2.

68 LT-Drs. 20/10752, S. 2.

69 Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (Sächsisches Informationssicherheitsgesetz – SächsISichG) vom 02.08.2019 (SächsGVBl. S. 630).

70 Zuletzt durch Artikel 2 Absatz 2 des Gesetzes vom 22.07.2024 (SächsGVBl. S. 706) und durch das Gesetz vom 05.07.2024 (SächsGVBl. S. 590) geändert.

Zugang über andere sichere Schnittstellen erfolgt. Der Informationssicherheitsbeauftragte des Landes kann nach § 5 Abs. 4 SächsiSichG gegenüber nicht-staatlichen Stellen im Benehmen mit dem Beauftragten für Informationssicherheit des Betreibers des Kommunalen Datennetzes Anordnungen treffen, um Gefahren für die informationstechnischen Systeme, die mit dem Kommunalen Datennetz verbunden sind, abzuwehren.

Auch der Informationsfluss zur Gewährleistung der IT-Sicherheit wurde in Sachsen angegangen. § 15 SächsISichG sieht eine stellenübergreifende Meldepflicht für staatliche und nicht-staatliche Stellen in Sachsen vor, die u.a. an das Kommunale Datennetz angeschlossen sind und denen Informationen bekannt werden, die zur Abwehr von Gefahren für die informationstechnischen Systeme von Bedeutung sind. Die Meldung muss an das Sicherheitsnotfallteam nach § 6 SächsISichG erstattet werden. Außerdem gilt die Meldepflicht des § 16 SächISichG für Sicherheitsereignisse und -vorfälle in den eigenen IT-Systemen nach § 17 SächsISichG auch für nicht-staatliche Stellen, die mit dem Sächsischen Verwaltungsnetz oder dem Kommunalen Datennetz verbunden sind.

Das Sächsische Informationssicherheitsgesetz wurde im Jahr 2024 bereits auf die Regelungen der NIS-2-Richtlinie vorbereitet und überarbeitet, die Änderungen gelten seit Oktober 2024. So wird der „Landes-CISO" nach § 5 Abs. 1 S. 1 Nr. 5 SächsISichG zur Aufsichtsbehörde im Sinne der NIS-2-Richtlinie.

**4) Saarländisches Informationssicherheitsgesetz**

Ebenfalls im Jahr 2019 trat das Saarländische Informationssicherheitsgesetz (IT-SiG SL)[71] in Kraft. Nach § 1 IT-SiG SL dient es der Informationssicherheit des Landesdatennetzes, der informationstechnischen Systeme, der genutzten Anwendungen und der darüber verarbeiteten Informationen der Behörden des Saarlandes und umfasst u.a. auch den Tätigkeitsbereich der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Bemerkenswert ist die gesetzgeberische Motivation, die neben dem Schutz sensibler Daten von Bürgerinnen und Bürgern selbstverständlich auch im Gebot der Aufrechterhaltung der Funktionsfähigkeit der öffentlichen Verwaltung liegt[72].

**Bemerkenswert ist die gesetzgeberische Motivation, die neben dem Schutz sensibler Daten von Bürgerinnen und Bürgern selbstverständlich auch im Gebot der Aufrechterhaltung der Funktionsfähigkeit der öffentlichen Verwaltung liegt.**

Das Gesetz referenziert für die behördenübergreifenden Pflichten in § 3 IT-SiG SL für die informationstechnischen Systeme der Behörden auf den Stand der Technik sowie die Vorgaben der DSGVO. Daher treffen die Behörden nach § 3 Abs. 1 S. 2 IT-SiG SL zu diesem Zweck angemessene technische und organisatorische Maßnahmen und erstellen die hierzu erforderlichen Informationssicherheitskonzepte. Sofern Behörden Informationen bekannt werden, die zur Abwehr von Gefahren für die Informationssicherheit von Bedeutung sind, unterrichten sie unverzüglich den zentralen IT-Dienstleister (IT-DLZ) des Landes hierüber.

§ 4 IT-SiG SL regelt eine Gefahrenabwehrbefugnis dieses zentralen IT-Dienstleisters. Hierfür ist auch eine Auswertung von Protokoll- und Inhaltsdaten nach §§ 5 f. IT-SiG SL sowie die darüber hinausgehende Auswertungsbefugnis bei besonderen Gefahren nach § 7 IT-SiG SL mit der dazugehörigen Benachrichtigungspflicht des § 9 IT-SiG SL gegenüber den Betroffenen sowie betroffenen Behörden gegeben. Außerdem wacht der Landesbeauftragte für den Datenschutz nach § 12 IT-SiG SL über die Auswertungen, indem diesem zur Kontrolle jährlich die erfolgten Verarbeitungen durch den zentralen IT-Dienstleister vorzulegen sind. Die Auswertungen nach §§ 4-7 IT-SiG SL verlangen gemäß § 8 IT-SiG vom zentralen IT-Dienstleister ein regelmäßig angepasstes Sicherheitskonzept.

Im Saarland wurde ebenfalls mit der Einführung des IT-SiG SL auch die Funktion eines Landes-CISO geschaffen. So kennt Anlage I in der Besoldungsgruppe B 5 zum SBesG das Amt „Direktor des Landesamtes für Zentrale Dienste - als Leiter des Landesamtes für

71 Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes (Informationssicherheitsgesetz Saarland - IT-SiG SL) v. 15.5.2019 (Amtsbl. I, S. 653 ff.).

72 Landtag des Saarlandes, LT-Drs. 16/761, S. 1.

Zentrale Dienste und Landesbeauftragter für Informationssicherheit“. Begründet wurde dies im Entwurf zum IT-SiG SL mit dem Bedarf zur Koordinierung und Steuerung der Aufgaben im Zusammenhang mit der Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur der Landesverwaltung.[73] Bemerkenswert ist nun aber, dass das IT-SiG SL die Stellung des Landes-CISO nicht weiter ausgestaltet, mit welchen Instrumenten er diesen Aufgaben nachkommen kann oder wie etwa seine Stellung geschützt und neutral bleibt. Gerade dies ist aber elementar, damit die auf die Hilfe des zentralen IT-Dienstleisters angewiesenen Gemeinden und Gemeindeverbände IT-sicher aufgestellt sein können. Denn diese sind auf die Unterstützungsaufgaben des zentralen IT-Dienstleisters angewiesen, der die Befähigung und auch den technischen Zugriff auf die IT-Kommunikationsdienste des Landes hat.

### 5) Bayerisches Digitalgesetz

Einen generelleren Weg über die Cybersicherheit hinaus ist der Freistaat Bayern gegangen. Dort trat im Jahr 2022 das Bayerische Digitalgesetz (BayDiG) in Kraft[74].

**Dieses thematisiert seinem Titel gemäß nicht nur die Informationssicherheit, sondern reguliert die gesamte Digitalisierung der Verwaltung.**

Dieses thematisiert seinem Titel gemäß nicht nur die Informationssicherheit, sondern reguliert die gesamte Digitalisierung der Verwaltung. Der Anwendungsbereich des Gesetzes erfasst nach Art. 1 Abs. 1 S. 1 BayDiG u.a. Gemeinden und Gemeindeverbände. Mit dem Gesetz soll die Digitalisierung des Staats und der Verwaltung gefördert werden, Art. 2, Art. 5 BayDiG. Wie dies konkret ausgestaltet sein soll, lässt sich im zweiten Teil des Gesetzes mit dem Titel „Digitale Verwaltung erkennen“. Zu den einzelnen Bausteilen zählen:

- Digitale Kommunikation und Dienste, Art. 16-18 BayDiG
- Digitales Verwaltungsverfahren, Art. 19-25 BayDiG
- Portalverbund Bayern, Art. 26-32 BayDiG
- Digitale Akten und Register, Art. 33-35 BayDiG
- Behördenzusammenarbeit und Rechenzentren, Art. 36-40 BayDiG

Der Dritte Teil des BayDiG (Art. 41-49c) widmet sich komplett der IT-Sicherheit. Danach existiert nach Art. 41 BayDiG ein Landesamt für Sicherheit in der Informationstechnik, dessen Aufgabenkatalog in Art. 42 BayDiG geregelt ist. Dieses unterstützt etwa alle an das Behördennetz angeschlossenen Stellen und entwickelt für diese sicherheitstechnische Mindeststandards, deren Einhaltung es dann auch überprüft. Außerdem übernimmt es Notfallaufgaben, wofür es die Aufgabe eines Computer-Notfallteams (CSIRT) i. S. d. NIS-2-Richtlinie übernimmt[75], Art. 42 Abs. 1 Nr. 7 BayDiG. Das Landesamt für Sicherheit in der Informationstechnik darf auch nach Art. 45 Abs. 1 S. 1 BayDiG die Sicherheit der Informationstechnik staatlicher und an das Behördennetz angeschlossener Stellen untersuchen und bewerten, zudem nach Abs. 2 auch die Untersuchung und Bewertung von auf dem Markt bereitgestellten oder zur Bereitstellung auf dem Markt vorgesehenen informationstechnischen Produkten und Systemen wahrnehmen.

Zu den in Art. 43 BayDiG genannten behördenübergreifenden Pflichten, die also auch Gemeinden und Gemeindeverbände treffen, zählt nach Abs. 3 die unverzügliche Unterrichtungspflicht bei Kenntnissen über Gefahren für die IT-Sicherheit an das Landesamt für Sicherheit in der Informationstechnik sowie die oberste Dienstbehörde der unterrichtenden Stelle.

### 6) Landesrechtliche Verwaltungsvorschriften zur NIS-2-Richtlinie

Neben gesetzlichen Vorgaben zur IT- und Cybersicherheit auf kommunaler Ebene haben sich manche Bundesländer auch für die Regelung über Verwaltungsvorschriften entschieden. Bei einer Verwaltungsvorschrift handelt es sich um generell-abstrakte, binnenrechtliche Regelungen ohne Außenwirkung gegenüber den Bürgern. Sie sind von einer vorgesetzten an eine nachgeordnete Stelle gerichtet und aufgrund der Weisungsgebundenheit von Beamten und öffentlichen Bediensteten bindend.[76]

73 Landtag des Saarlandes, LT-Drs. 16/761, S. 32.
74 Gesetz über die Digitalisierung im Freistaat Bayern (Bayerisches Digitalgesetz – BayDiG) v. 22.7.2022 (GVBl. S. 374).
75 Eine weitere Neuerung zur Adaption der NIS-2-Richtlinie sind die Art. 49a-49c BayDiG für Einrichtungen mit einer besonderen Bedeutung für den Binnenmarkt.
76 Erbguth/Guckelberger, Allgemeines Verwaltungsrecht, § 7 Rn. 8.

Das Land Niedersachsen hat im Oktober 2024 nach eigenen Angaben die NIS-2-Richtlinie umgesetzt, indem die Landesregierung eine neue Verwaltungsvorschriftsschrift erlassen hat, die das Ministerium für Inneres und Sport als zuständige Behörde für Cybersicherheit sowie das Niedersachsen-CERT als Computer-Notfallteam benannt hat. Mit der neuen Verwaltungsvorschrift sollen die Sicherheitsstandards für Netz- und Informationssysteme in den besonders kritischen Teilen der Landesverwaltung erheblich verbessert und der bereits seit 2019 bestehende Rechtsrahmen des Niedersächsischen Gesetzes über digitale Verwaltung und Informationssicherheit (NDIG[77]) um europarechtliche Vorgaben ergänzt werden.[78] Mit dem NDIG wurde in § 2 NDIG auch für Niedersachsen eine Position des IT-Bevollmächtigten der Landesregierung zur Koordination des Einsatzes der Informationstechnik durch das Land und die Fortentwicklung der digitalen Verwaltung geschaffen.

Ähnliches geschah im Oktober 2024 in Rheinland-Pfalz. Auch hier wurde u.a. eine Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie erarbeitet. Aus der Sitzung des Ministerrates im März 2024 lässt sich erkennen, dass sich die Vorschrift nur auf die unmittelbare Landesverwaltung bezieht. Zudem sollte eine Cybersicherheitsstrategie erstellt und das vom IT-Planungsrat verabschiedete, deutschlandweit einheitliche Identifizierungskonzept auf die unmittelbare Landesverwaltung angewendet werden.[79]

**Zwischenfazit**

Nachdem Gemeinden über die Kritis-Gesetzgebung des Bundes nur in Ausnahmefällen über den Betrieb von Unternehmen und Einrichtungen zu Schutzvorkehrungen für ihre IT-Prozesse verpflichtet werden, wird auf Länderebene ein etwas engmaschigeres Netz gesponnen. Eine Reihe an Ländern sind die Bedeutung des Problemkomplexes IT-Sicherheit zumindest angegangen und haben entweder IT-Sicherheits-, Cybersicherheits- oder Digitalisierungsgesetze mit entsprechenden Schwerpunkten erlassen. Vordergründig richten sich diese zwar an die Länderinstitutionen, aber auch Gemeinden und Gemeindeverbände werden in Teilen erfasst. Im Zusammenhang mit der NIS-2-Richtlinie wurden weiterhin auch (teilweise die Ländergesetze ergänzende) Verwaltungsvorschriften zur Steigerung der Vorgaben der IT-Sicherheit erlassen, die sich aber nur an die landesunmittelbare Verwaltung richten. Aufgrund ihrer Binnenwirkung dürften sie regelmäßig auch für Vorgaben an Gemeinden außerhalb von weisungsgebundenen Pflichtaufgaben ausscheiden.

Sinnvollerweise etablieren die Ländergesetze einen Landes-CISO als Beauftragten für die IT-Sicherheit, der teilweise unterschiedlich benannt wird. Dem Landes-CISO kommen häufig Aufgaben bei der Standardisierung von IT-Sicherheitsvorgaben sowie der Überwachung von deren Einhaltung und auch der Beratung von Behörden und Gemeinden bzw. Gemeindeverbänden zu.

Für IT-Sicherheitsgefährdungen verpflichten die Ländergesetze die Normadressaten zur Unterrichtung entweder an den Landes-CISO oder dessen übergeordneter Stelle. Kommt es dennoch zu einem Cyber Incident, bieten die Landes-CSIRTs u.a. für die Gemeinden und Gemeindeverbände Unterstützungsmaßnahmen im Notfall an.

Betrachtet man aber insgesamt die Cybersicherheitsarchitektur in Deutschland, besteht gerade auf der Ebene der Länder und Kommunen der Eindruck eines unübersichtlichen und nicht stringent durchregulierten Verwaltungsgefüges fort[80], das die jeweiligen Aufgaben der staatlichen Stellen und damit auch Ansprechpartner für die Kommunen schwer überschaubar macht. Eine solche Vielzahl an unterschiedlichen Anlaufstellen schwächt im Ergebnis die Umsetzung kommunaler Cybersicherheitsbemühungen.

**Eine solche Vielzahl an unterschiedlichen Anlaufstellen schwächt im Ergebnis die Umsetzung kommunaler Cybersicherheitsbemühungen.**

77 Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) v. 24.10.2019 (Nds. GVBl. S. 291).

78 ur Pressemeldung: https://www.stk.niedersachsen.de/startseite/presseinformationen/niedersachsen-setzt-nis-2-richtlinie-erfolgreich-um-starkung-der-cyber-sicherheit-in-der-verwaltung-236776.html.

79 Sitzung des Ministerrates am 19. März 2024 „TOP 4: Umsetzung der NIS-2-Richtlinie in Rheinland-Pfalz“, abrufbar unter: https://tpp.rlp.de/eakte/coo-2298-102-4-2285135/resource/274ae923-bcc3-4c5e-935f-1c36e1d2a306?inner_span=True.

80 „Deutschlands staatliche Cybersicherheitsarchitektur“, Stiftung Neue Verantwortung, 2019, S. 16.

# Teil 4
# Verbesserungspotenzial

Wenngleich nun also sowohl der Bundes- als auch die Landesgesetzgeber vielfach schon tätig geworden sind, ergeben sich für die Cybersicherheitsvorgaben der Kommunen und Gemeindeverbände nach wie vor erhebliche Verbesserungspotenziale, die nachfolgend aufgezeigt werden.

**Wer muss reagieren?**
Betrachtet man nun das Verbesserungspotenzial bei der kommunalen Cybersicherheits-Regulierung, stellt sich zunächst die Frage, wer denn am Zuge ist, um Veränderungen auf gesetzlicher Ebene anzustoßen und vorzunehmen. Der Bund stützt seine Gesetzgebungskompetenzen für die NIS-2-Gesetzgebung, wobei hier nicht nur Änderungen am BSIG, sondern bspw. auch am TKG oder EnWG vorgenommen werden, auf Art. 73 Abs. 1 Nr. 7 GG (Telekommunikation) sowie auf Art. 74 Abs. 1 Nr. 11 GG (Recht der Wirtschaft, einschließlich gefahrenabwehrrechtlicher Annexkompetenz) in Verbindung mit Art. 72 Abs. 2 GG und Art. 74 Abs. 1 Nr. 12 GG (Sozialversicherung einschließlich der Arbeitslosenversicherung). Eine bundesgesetzliche Regelung dieser Materie sei zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich, da eine Regelung durch den Landesgesetzgeber zu erheblichen Nachteilen für die Gesamtwirtschaft führen würde, die sowohl im Interesse des Bundes als auch der Länder nicht hingenommen werden könnten. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte, z. B. unterschiedliche Voraussetzungen für die Vergabe von Sicherheitszertifikaten, erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten.[81]

Soweit sich der Bundesgesetzgeber folglich nicht ausnahmsweise auf eine ausschließliche oder konkurrierende Gesetzgebungskompetenz stützen kann, liegt es in der Gesetzgebungskompetenz der Länder, Regelungen zu erlassen. Hierbei ist nun aber bei der

> **Soweit sich der Bundesgesetzgeber folglich nicht ausnahmsweise auf eine ausschließliche oder konkurrierende Gesetzgebungskompetenz stützen kann, liegt es in der Gesetzgebungskompetenz der Länder, Regelungen zu erlassen.**

kommunalen Cybersicherheitsregulierung die kommunale Selbstverwaltungsgarantie aus Art. 28 Abs. 2 S. 1 GG zu beachten. Diese Garantie verbietet Eingriffe in den Kernbereich der kommunalen Selbstverwaltung. Außerhalb dieses Kernbereichs sind Eingriffe auf Grundlage eines Gesetzes möglich, sofern der Verhältnismäßigkeitsgrundsatz gewahrt wird.[82] Bezüglich der IT-Standardisierungen wird diesbezüglich zurecht darauf hingewiesen, dass solche Regelungen stets mit Angemessenheitsklauseln (wie etwa in § 8a Abs. 1 BSIG bzw. § 30 Abs. 1 BSIG-E und Art. 32 DSGVO) auskommen, die in der Angemessenheitsabwägung auch die Umsetzungskosten berücksichtigen.[83] Auch das verfassungsrechtlich garantierte Konnexitätsprinzip (bspw. Art. 78 Abs. 3 LVerf NRW) spricht nicht grundsätzlich gegen Cybersicherheitsvorgaben für Kommunen, zumal es sich bei solchen Digitalisierungsvorgaben um keine Sachaufgaben handelt, was das Argument des Konnexitätsprinzips gegen entsprechende Vorgaben deutlich schwächt.[84]

81 BT-Drs. 20/13184, S. 91.
82 Ziegler, DSRITB 2023, 349 (352 f.) m.w.N.
83 Ziegler, DSRITB 2023, 349 (353) m.w.N.
84 Ziegler, DSRITB 2023, 349 (355 f.) m.w.N.

Den Ländern steht also die Kompetenz zu, Gesetze zur Steigerung der Cybersicherheit für die kommunale Ebene zu erlassen, selbstverständlich unter Wahrung der einschränkenden Vorgaben u.a. aus Art. 28 Abs. 2 S. 1 GG. Gerade mit dem Hintergrund der staatlichen Cybersicherheitsarchitektur in Deutschland ist es nahezu die Pflicht der Länder, hier noch einmal einen deutlichen politischen und auch juristischen „Schwung" mitzunehmen, um die Cybersicherheit der Kommunen nachhaltig verbessern zu können. Denn ein Abwarten etwa auf den Bund ist hier schädlich – welcher wiederum selbst verpflichtet ist, beispielsweise die Vorgaben aus NIS-2 bundeseinheitlich zu realisieren. Gesetzliche Vorgaben für die Kommunen unter Wahrung der Selbstverwaltungsgarantie bei einer gleichzeitigen Verringerung der Zahl unterschiedlichster staatlicher Anlaufstellen für die Cybersicherheit sind also dringend erforderlich.

> **Gesetzliche Vorgaben für die Kommunen unter Wahrung der Selbstverwaltungsgarantie bei einer gleichzeitigen Verringerung der Zahl unterschiedlichster staatlicher Anlaufstellen für die Cybersicherheit sind also dringend erforderlich.**

**EU-Cybersicherheitsstrategie und Kommunen**
Sinnvollerweise sieht die EU-Cybersicherheitsstrategie einen All-Gefahren-Ansatz vor und berücksichtigt die cyberbezogenen und die physischen Risiken, sie nimmt damit einen modernen Blickwinkel auf kontinuitätsbeeinträchtigende Ereignisse ein. Wie eingangs erwähnt, hat sich zumindest der IT-Planungsrat gegen eine unmittelbare Verpflichtung lokaler Ebenen im Hinblick auf die NIS-2-Gesetzgebung ausgesprochen. Die bisherigen Entwürfe zum NIS2UmsuCG folgten dieser Empfehlung, es ist daher nicht zu erwarten, dass bei der flächendeckend in der kommenden Legislaturperiode erfolgenden NIS-2-Umsetzung in Deutschland eine Einbeziehung der Kommunen erfolgen wird.[85] An dieser Stelle kann damit der Hinweis erneuert werden, dass es vielmehr in den Händen der Länder liegt, sich und die Kommunen cyberresilient aufzustellen. Zutreffend sind daher schon Sachsen, Bayern, Niedersachsen und Rheinland-Pfalz mit gutem Beispiel vorangegangen und haben die NIS-2-Vorgaben umgesetzt.

Gleichzeitig kann man aber ebenso feststellen, dass keines der Bundesländer den „All-Gefahren-Ansatz" der EU-Cybersicherheitsstrategie bereits befolgt hat. Während man die Unternehmen in Europa also auf eine hybride Gefährdungslage vorbereiten will, liegt der Fokus der Länder, teilweise auch unter dem Deckmantel des Begriffs der „Cybersicherheit", allein auf der IT-Sicherheit. Hier muss dringend nachgebessert werden, gerade wenn man berücksichtigt, dass die Initiierung von Sicherheitsprozessen im öffentlichen Umfeld noch länger Zeit in Anspruch nimmt als in der Privatwirtschaft, weil bspw. vergaberechtliche Verfahren eingehalten und Haushaltsmittel erwirkt werden müssen.

**Inhaltliches Verbesserungspotenzial**
Neben der eben erwähnten strategischen Ausrichtung von Vorgaben müssen diese vor allem auch inhaltlich nachgeschärft werden. Hier fallen mehrere Säulen auf, die den Kommunen und Gemeindeverbänden Halt geben können.

Es ist sinnvoll, wie bereits schon vielfach geschehen, einen Landes-CISO zu etablieren. Dieser verfolgt standardisierende, überwachende, aber auch beratende Aufgaben. Allerdings fehlt es den bisherigen Gesetzen an einer ausreichend unabhängigen Stellung des Landes-CISO. Mit anderen Worten: so wie der Landes-CISO in den Gesetzen vorgesehen ist, würde er keiner Auditierung in einem Unternehmen standhalten. Es gehört auch zu den Aufgaben eines CISO, unangenehm zu sein. Hierfür muss die Unabhängigkeit gewahrt sein, sei es vor aufsichtsrechtlichem Einschreiten, aber auch vor beamten- oder arbeitsrechtlichen Konsequenzen. Außerdem ist es ebenso erforderlich, dass das Aufgabenspektrum des Landes-CISO klar

> **Es ist sinnvoll, wie bereits schon vielfach geschehen, einen Landes-CISO zu etablieren. Dieser verfolgt standardisierende, überwachende, aber auch beratende Aufgaben.**

85 Andere Staaten in der EU handhaben dies im Rahmen ihrer nationalen Umsetzung von NIS-2 durchaus auch anders, so zum Beispiel Kroatien, Zypern, Litauen oder Rumänien.

festgelegt ist, damit er sich bei Kompetenzfragen mit einer rechtssicheren Position Gehör verschaffen kann. Allein einen Landes-CISO als Besoldungsstufe einzuführen und ihn an die Spitze eines Landes-IT-Dienstleisters zu stellen, ist ungenügend.

**Außerdem sind Standardisierungen von Sicherheits-Management-Prozessen sinnvoll und nicht nur dann, wenn bestimmte Landes-IT-Prozesse genutzt werden, sondern für das gesamte Handeln der kommunalen Verwaltung.**

Außerdem sind Standardisierungen von Sicherheits-Management-Prozessen sinnvoll und nicht nur dann, wenn bestimmte Landes-IT-Prozesse genutzt werden, sondern für das gesamte Handeln der kommunalen Verwaltung. Es existiert etwa das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ des BSI, das an den BSI-Standard 200-2 angelehnt ist.[86] Solche Standardisierungen können auch zu Kostenreduzierungen in der Realisierung kommunaler Cybersicherheit führen. Wenn häufig das Kostenargument gegen Cybersicherheit eingesetzt wird, so kann man diese Argumentation auch umkehren: Für einen externen IT-Dienstleister sinken die Kosten, wenn flächendeckend gleiche Sicherheitsstandards gelten, auf die er sich beim Roll-Out seines Produkts einstellen kann. Vielmehr noch sogar: fehlende Standardisierungen können fachkundige Unternehmen abschrecken, sich auf den öffentlichen Markt zu konzentrieren, weil allein schon in der Analyse des Flickenteppichs unterschiedlicher Regelungen wertvolle Zeit und Einsparpotenziale verlorengehen, ohne überhaupt mit der Konzeption von Produkten auf unterschiedliche Standardsierungen begonnen zu haben.

Richtigerweise setzt man auf Landesebene auf Notfall-Teams. Diese müssen auch den Kommunen zur Hilfe eilen. Denn, je nach Größe der Kommune, dürfte es eine finanzielle und personelle Überforderung darstellen, komplette eigene kommunale IT-Notfall-Teams vorzuhalten. Hier müssen Synergien genutzt werden.

86 Das Grundschutz-Profil ist abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html.

# Teil 5
# Best Practice-Hinweise für Kommunen

Nach diesen Ausführungen wird deutlich, dass die Cybersicherheit von Kommunen stark auch mit ihrer juristischen Einbettung zusammenhängt. Mit juristischen Vorgaben finden sich für Kommunen bessere Argumente, um die Finanzierung von Cybersicherheitsmaßnahmen voranzutreiben. Dennoch dürfen sich Kommunen, auch wenn sie vor der Herausforderung der finanziellen Deckung von Cybersicherheitsprozessen stehen, nicht hinter dieser Hürde verstecken. Zugleich stellen die Ausgaben nicht die einzige Stellschraube zur Cyberresilienz dar, erforderlich sind vielmehr eine etablierte Cybersicherheitskultur und strukturierte Prozesse. Hierfür helfen u.a. das IT-Grundschutz-Profil zur

> **Zugleich stellen die Ausgaben nicht die einzige Stellschraube zur Cyberresilienz dar, erforderlich sind vielmehr eine etablierte Cybersicherheitskultur und strukturierte Prozesse.**

Basis-Absicherung der Kommunalverwaltung des BSI und auch die Empfehlungen der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrats. Mithilfe dieser Mindeststandards lassen sich nachfolgend mehrere Best Practice-Maßstäbe für Kommunen aufstellen.

### Cybersicherheit als Leitungsaufgabe in Kommunalverwaltungen

Auch für Kommunen gilt wie in der Wirtschaft der Grundsatz, dass es sich bei der Cybersicherheit um eine Leitungsaufgabe handelt. Die „Basis-Absicherung Kommunalverwaltung" basiert auf dem BSI-Standard 200-2 (IT-Grundschutz-Methodik). Dieser stellt darauf ab, dass die Leitungsebene die Verantwortung trägt, dass „alle Geschäftsbereiche zielgerichtet und ordnungsgemäß funktionieren und dass Risiken frühzeitig erkannt und minimiert werden.[87]". Die entscheidenden Kommunalorgane müssen entsprechend dem „Tone-from-the-Top-Prinzip" die Bedeutung der Cybersicherheit in der Kommune vorleben und sie mit der ausreichenden Ernsthaftigkeit und finanziellen Ausstattung initiieren. Dadurch wird das Vertrauen von Bürgerinnen und Bürgern sowie Unternehmen in den Staat und die für sie im Alltag unmittelbare spürbare Kommune gestärkt[88]. Möglicherweise stellt eine resilient-digitalisierte Kommune in Zukunft gar einen Wettbewerbsvorteil zur Ansiedelung von Unternehmen dar. Zuletzt verlangt auch der Grundsatz sparsamen Haushaltens einen sorgsamen Umgang mit öffentlichen Geldern. Die Schäden durch Cyber Incidents übersteigen im Nachgang meist deutlich die Kosten, die für die Prävention vor einem Incident notwendig gewesen wären. Von der

> **Die Schäden durch Cyber Incidents übersteigen im Nachgang meist deutlich die Kosten, die für die Prävention vor einem Incident notwendig gewesen wären.**

Leitungsebene aus müssen daher professionelle und standardisierte Cybersicherheitsprozesse initiiert werden. Hilfestellungen für Standardisierungen existieren durchaus, so etwa eine „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen"[89]. Solche zur Verfügung stehenden Standards sollten unbedingt aufgegriffen werden.

87 „BSI-Standard 200-2: IT-Grundschutz-Methodik" des BSI, S. 20; „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung" des BSI, S. 3 und S. 10.

88 Vgl. hierzu die Pressemittelung des Ministeriums für Infrastruktur und Digitales des Landes Sachsen-Anhalt vom 26.10.2024 zum Projekt „SicherKommunal in Sachsen-Anhalt".

89 „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen" des IT-SiBe-Forums.

### Berücksichtigung des All-Gefahren-Ansatzes

Die EU hat es mit ihrer Cybersicherheitsstrategie vorgelebt: Kommunen müssen einen „All-Gefahren-Ansatz" berücksichtigen. Das bedeutet, dass allein ein Fokus auf die IT-Sicherheit, ggf. unter dem Deckmantel des Begriffs der Cybersicherheit, nicht ausreicht, um eine Kommune mit ihren Einrichtungen nachhaltig resilient zu gestalten. Denn in der hybriden Gefährdungslage lassen sich die Risiken für die Funktionsfähigkeit einer Kommune (in Anlehnung an die Business Continuity auch als „Public Sector Continuity" bezeichnet) nicht mehr klar einer cyberbezogenen oder nicht-cyberbezogenen Risikoherkunft zuordnen. In Zeiten von Sabotageakten, Terror- und Cyberattacken und Umweltereignissen, die auch Kommunen treffen können, müssen folglich ganzheitliche Risikomanagement-Prozesse etabliert werden, die nicht nur einseitig auf den Risikobereich der IT-Sicherheit blicken.

### Kommunaler CISO

Auch wenn die Letztverantwortung für die Cybersicherheit stets bei der Leitung der Kommune verbleibt, ist aufgrund der Begrenztheit der fachlichen und zeitlichen Ressourcen eine Delegation von Cybersicherheits-Aufgaben an eine Fachperson oder Fachabteilung, je nach Größe der Kommune, unumgänglich und üblich. Zwar muss von der Leitungsebene auch eine fachliche Expertise bezüglich der Gefahren aus dem Cyberbereich erwartet werden – die NIS-2-Richtlinie schreibt daher für Leitungspersonen von Kritis-Unternehmen künftig auch ausdrücklich Schulungen vor[90] – dennoch steht und fällt die Cybersicherheit mit einem kundigen Chief Information Security Officer (CISO) – der BSI-Standard 200-1 verwendet alternativ auch den Begriff des Informationssicherheitsbeauftragten (ISB)[91]. Erforderlich ist demgemäß nicht nur die Schaffung von „Landes-CISO", wie in einigen Ländern gesetzlich schon geschehen, sondern auch von „Kommunal-CISO". Diese CISO können mit ihren Fachkenntnissen vor allem auch die zwingend notwendige Awareness innerhalb der Kommune stärken, um durch menschliche Fehler entstehende Risiken zu verringern, etwa durch Schulungen oder eLearning-Programme[92]. Da zugleich aber auch

> **Diese CISO können mit ihren Fachkenntnissen vor allem auch die zwingend notwendige Awareness innerhalb der Kommune stärken, um durch menschliche Fehler entstehende Risiken zu verringern, etwa durch Schulungen oder eLearning-Programme.**

die personellen und finanziellen Ressourcen von Kommunen berücksichtigt werden müssen, gestattet die „Basis-Absicherung Kommunalverwaltung" bei der Organisationsstruktur, dass eine Person, soweit dies wirtschaftlich notwendig ist, auch mehrere Verantwortlichkeiten auf sich vereinen kann[93], wovon sonst aufgrund von Interessenskonflikten und Überlastungen abzuraten ist.

### Resilientes Outsourcing im IT-Bereich

Wie auch in der freien Wirtschaft ist es bei Kommunen ebenso üblich, dass externe IT-Lösungen genutzt werden, weil eigene Ressourcen hierfür nicht vorhanden oder ausreichend sind. Auch beim Outsourcing sind wiederum verschiedene Ausmaße möglich. Es existieren in vielen Bundesländern große kommunale IT-Zweckverbände. Andernorts gibt es deutlich kleinere Zusammenschlüsse von Kommunen. Das Ausmaß eines Ausfalls eines großen IT-Zweckverbands wurde bereits eingangs anhand des Beispiels SIT beleuchtet. Für viele Kommunen führt aber am Outsourcing mangels eigener Ressourcen kein anderer Weg vorbei. Daher ist es notwendig, ein verantwortungsvolles Outsourcing zu betreiben.

90 Kipker/Dittrich, MMR 2023, 481 (486).
91 „BSI-Standard 200-2: IT-Grundschutz-Methodik" des BSI, S. 12.
92 Vgl. zur Bedeutung dieser Elemente für die Kommunen: Pressemitteilung des Hessischen Ministeriums des Innern, für Sicherheit und Heimatschutz vom 03.01.2025.
93 „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung" des BSI, S. 11.

Eine falsche Annahme ist darin zu sehen, allein durch Outsourcing sämtliche IT-Gefahren beseitigen zu können. Denn auch hier ist wieder an die Letztverantwortung der Leitungsebene von Kommunen zu erinnern, die keine vollständige Delegation von Verantwortlichkeiten zulässt. Die verantwortlichen IT-Dienstleister, unabhängig davon, ob es sich um kommunale Zusammenschlüsse oder externe Unternehmen handelt, müssen ausreichend zertifiziert sein. Zudem

> **Die verantwortlichen IT-Dienstleister, unabhängig davon, ob es sich um kommunale Zusammenschlüsse oder externe Unternehmen handelt, müssen ausreichend zertifiziert sein.**

müssen im Sinne der Absicherung der digitalen Lieferkette unbedingt Redundanzen vorgehalten werden, falls ein Dienstleister ausfällt.

### Vorbereitung auf den IT-Notfall

Die besten Cybersicherheitsmaßnahmen führen niemals zu einer einhundertprozentigen Cybersicherheit – es wird stets zu Vorfällen kommen.

> **Die besten Cybersicherheitsmaßnahmen führen niemals zu einer einhundertprozentigen Cybersicherheit – es wird stets zu Vorfällen kommen.**

Dennoch ist es notwendig, die Folgen von IT-Sicherheitsvorfällen planvoll steuernd in das Risikomanagement einzubeziehen. Daher ist es unerlässlich, sich in der „Ruhephase“ auf einen solchen Notfall vorzubereiten. Denn die Planung erst in der „Stressphase“ ist zu spät. Die Letztverantwortung für die Notfallkonzeption liegt abermals bei der Leitungsebene der Kommune. Umgesetzt werden kann sie mittels des CISO. Erforderlich ist die Planung der Krise sowie die Übung der Krise. Sowohl Kommunen als auch Landkreise müssen demgemäß regelmäßige Übungen von Krisenereignissen durchführen. Die Abteilungen und Geschäftsbereiche der Kommunen und Landkreise müssen wissen, was im Ernstfall zu tun ist. Es müssen in der Planung der Krise die besonders relevanten Prozesse, weil hier bspw. Geldzahlungen im Sozialbereich erfolgen, evaluiert und priorisiert geschützt werden. Hilfestellungen ergeben sich über den BSI-Standard 200-2.

## Literatur


- Epping/Hillgruber, BeckOK GG, 58. Edition, 2024
- Dickmann/Vettermann, Geheimhaltung als Grundrechtsverletzung - Entscheidung des BVerfG zum Umgang von Behörden mit IT-Schwachstellen, MMR 2022, 740
- Dürig/Herzog/Scholz, GG, 103. EL Januar 2024
- Herpig/Dutke, Deutschlands staatliche Cybersicherheitsarchitektur, 11. Auflage 2023, Stiftung Neue Verantwortung (abrufbar unter: https://www.interface-eu.org/publications/deutschlands-staatliche-cybersicherheitsarchitektur, zuletzt abgerufen am: 06.01.2025)
- Kipker, Cybersecurity, 2. Auflage, 2023
- Kipker/Dittrich, Kritischer Infrastrukturschutz ganz konkret? Das KRITIS-Dachgesetz zur Umsetzung der neuen EU Resilienz-Richtlinie, ZRP 2023, 230
- Kipker/Dittrich, Rolle der Kritischen Infrastrukturen nach dem neuen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, MMR 2023, 481
- Kipker/Reusch/Ritter, Recht der Informationssicherheit, 1. Auflage 2023
- Dittrich/Dochow/Ippach, Rechtshandbuch Cybersicherheit im Gesundheitswesen, 1. Auflage 2024
- Denkhaus/Richter/Bostelmann, E-Government-Gesetz/Onlinezugangsgesetz, 1. Auflage 2019
- Erbguth/Guckelberger, Allgemeines Verwaltungsrecht, 10. Aufl. 2020
- Herrmann/Stöber, Das Onlinezugangsgesetz des Bundes – Wie der Gang zum Amt überflüssig werden soll, NVwZ 2017, 1401
- Irmscher, Risikobasierter Ansatz als regulatorischer Trend – auch bei kritischer Infrastruktur, ZRP 2024, 158.
- Martini/Botta, Kommunalverwaltung als Kritische Infrastruktur - Herausforderungen bei der Umsetzung der NIS-2-Richtlinie, LKV 2024, 293.
- Rüdebusch, Rolle der Kommunen im Rahmen der Digitalisierung, KommJur 2020, 41
- Vogel/Ziegler, Kritikalität: Von der BSI-KritisV zur NIS2-Richtlinie, International Cybersecurity Law Review (ICLR) 1/2023, 1
- Ziegler, Kommunale Cybersicherheit: Ist der Staat handlungsfähig?, Tagesspiegel Background Cybersicherheit v. 29.02.2024, abrufbar unter: https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/kommunale-cybersicherheit-ist-der-staat-handlungsfaehig (zuletzt abgerufen am: 06.01.2025).
- Ziegler, Verbindliche Mindeststandards kommunaler IT-Sicherheit, DSRITB 2023, 349


## Öffentlich abrufbare Dokumente


- „Die Lage der IT-Sicherheit in Deutschland 2024“ des BSI, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html (zuletzt abgerufen am: 06.01.2025)
- „Die Lage der IT-Sicherheit in Deutschland 2023“ des BSI, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html (zuletzt abgerufen am: 06.01.2025)
- „Die Lage der IT-Sicherheit in Deutschland 2022“ des BSI, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=1073198 (zuletzt abgerufen am: 06.01.2025)
- „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung“ des BSI, Stand: 13.11.2023, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html (zuletzt abgerufen am: 06.01.2025).
- „„BSI-Standard 200-2: IT-Grundschutz-Methodik“ des BSI, Version 1.0, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html?nn=128640 (zuletzt abgerufen am: 06.01.2025)
- „Abschlussbericht Security Incident – Südwestfalen-IT“, abrufbar unter: https://notfallseite.sit.nrw/aktuelle-meldungen?tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Bnews%5D=774&cHash=c9a93ee75846ddc335c34a3cbf61ae76 (zuletzt abgerufen am: 06.01.2025)
- „Tätigkeitsbericht Datenschutz 2023“ der Landesbeauftragten für Datenschutz und Akteneinsicht Bran-

denburg, abrufbar unter: https://www.lda.brandenburg.de/lda/de/service/taetigkeitsberichte/ (zuletzt abgerufen am: 06.01.2025).

- „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ des IT-Planungsrats, Stand 2018, abrufbar unter: https://www.it-planungsrat.de/fileadmin/beschluesse/2019/Beschluss2019-04_TOP12_Anlage_Leitlinie.pdf (zuletzt abgerufen am: 06.01.2025).
- „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen“ des IT-SiBe-Forums, Februar 2017, abrufbar unter: https://info.it-sibe-forum.de/dokumente/handreichung (zuletzt abgerufen am: 06.01.2025).

### Weitere Dokumente

- „BMI rettet die fristgemäße Umsetzung des OZG durch schwächstmögliche Verordnung zur IT-Sicherheit“, AG KRITIS, abrufbar unter: https://ag.kritis.info/2022/01/25/bmi-rettet-die-fristgemaesse-umsetzung-des-ozg-durch-schwaechstmoegliche-verordnung-zur-it-sicherheit/ (zuletzt abgerufen am: 06.01.2025).
- Pressemitteilung 187/2024 des Ministeriums für Infrastruktur und Digitales, Sachsen-Anhalt, 26.10.2024, abrufbar unter: https://mid.sachsen-anhalt.de/fileadmin/tsa_rssinclude/ministerium-fuer-infrastruktur-und-digitales_26_10_2024_pressemitteilung_sachsen-anhalt-startet-pilotprojekt-zur-erhoehung-der-it-und-informationssicherheit-in-den-kommunen.pdf (zuletzt abgerufen am: 06.01.2025).
- Pressemitteilung „Cybersicherheit in Hessen: Gefährdungslage 2024 weiterhin hoch“ des Hessischen Ministeriums des Innern, für Sicherheit und Heimatschutz vom 03.01.2025, abrufbar unter: https://hessen.de/presse/cybersicherheit-in-hessen-gefaehrdungslage-2024-weiterhin-hoch#:~:text=Cybersicherheit-,Cybersicherheit%20in%20Hessen%3A%20Gef%C3%A4hrdungslage%202024%20weiterhin%20hoch,Hessischen%20Innenministerium%20gegr%C3%BCndete%20Hessen3C%20zust%C3%A4ndig (zuletzt abgerufen am: 06.01.2025).

## Über das CII

Neue Zeiten brauchen eine neue Form der Forschung: das cyberintelligence.institute (CII) – ein Ort, an dem sich Innovation, Technologie, Strategie und Resilienz treffen. An der Schnittstelle von Wirtschaft und Wissenschaft, NGO und Start-up entwickelt das CII in Frankfurt am Main neue Lösungen für eine sichere digitale Zukunft. Kerngedanken sind die Kooperation, der Dialog und der interdisziplinäre und globale Informations- und Wissensaustausch, um Staat, Wirtschaft und Gesellschaft resilienter zu machen. Gefragt sind dabei ganzheitliche Konzepte, die Cybersicherheit nicht nur als abstrakte technisch-organisatorische Gewährleistungsverantwortung, sondern als gesamtgesellschaftliche Aufgabe zum Schutz gemeinsamer europäischer Werte verstehen. Damit tritt das cyberintelligence.institute aktiv für mehr digitale Sicherheit in einem Zeitalter neuer digitaler Herausforderungen ein.

Weitere Informationen gibt es auf der Website des CII unter www.cyberintelligence.institute.




**cyberintelligence.institute**
MesseTurm
Friedrich-Ebert-Anlage 49
D-60308 Frankfurt am Main

www.cyberintelligence.institute
info@cyberintelligence.institute

+49 69 505034602

---



Date of Publication: 03/2025